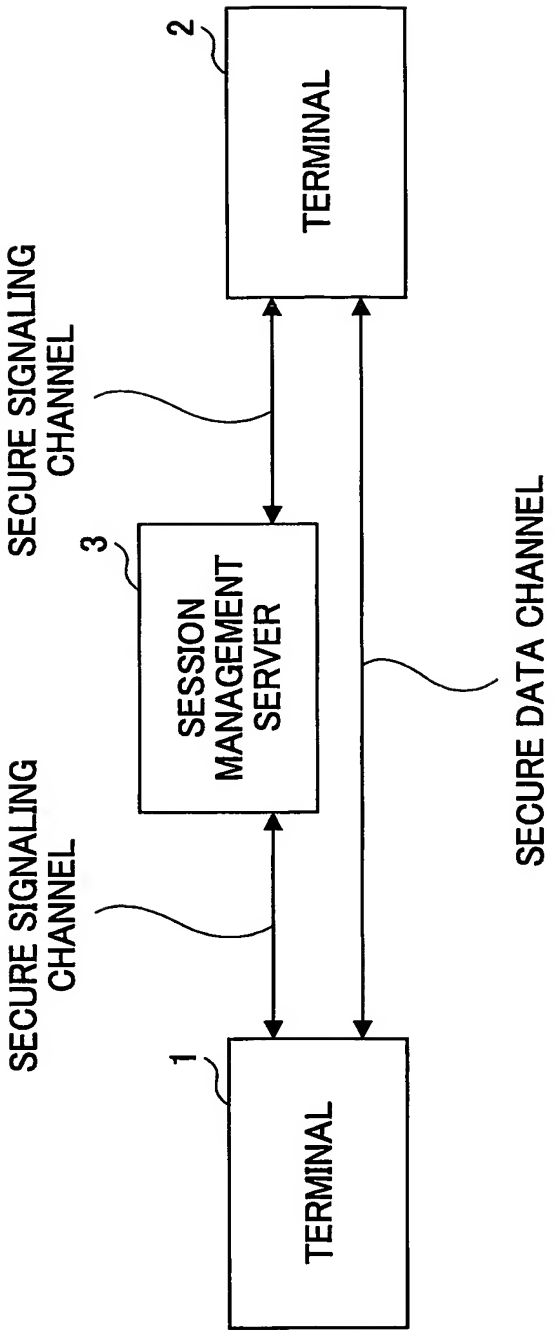
FIG.1


2
TERMINAL
SECURE SIGNALING CHANNEL
3
SESSION MANAGEMENT SERVER
SECURE SIGNALING CHANNEL
SECURE DATA CHANNEL
1
TERMINAL

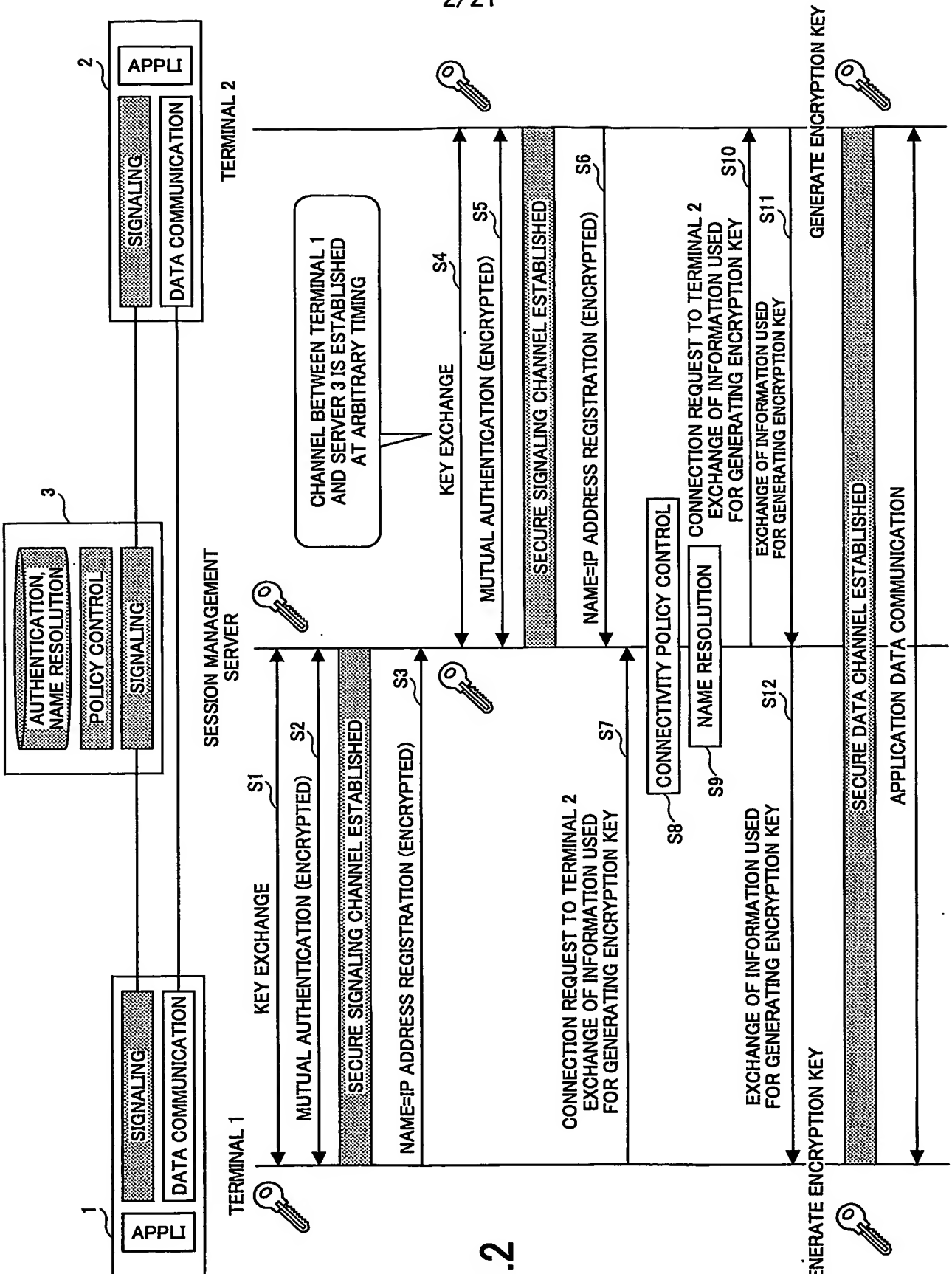

1
APPLI
SIGNALING
DATA COMMUNICATION
2
APPLI
SIGNALING
DATA COMMUNICATION
3
AUTHENTICATION, NAME RESOLUTION
POLICY CONTROL
SIGNALING
TERMINAL 1
SESSION MANAGEMENT SERVER
TERMINAL 2
CHANNEL BETWEEN TERMINAL 1 AND SERVER 3 IS ESTABLISHED AT ARBITRARY TIMING
KEY EXCHANGE
S1
MUTUAL AUTHENTICATION (ENCRYPTED)
S2
SECURE SIGNALING CHANNEL ESTABLISHED
NAME=IP ADDRESS REGISTRATION (ENCRYPTED)
S3
KEY EXCHANGE
S4
MUTUAL AUTHENTICATION (ENCRYPTED)
S5
SECURE SIGNALING CHANNEL ESTABLISHED
NAME=IP ADDRESS REGISTRATION (ENCRYPTED)
S6
CONNECTION REQUEST TO TERMINAL 2 EXCHANGE OF INFORMATION USED FOR GENERATING ENCRYPTION KEY
S7
CONNECTIVITY POLICY CONTROL
S8
NAME RESOLUTION
S9
CONNECTION REQUEST TO TERMINAL 2 EXCHANGE OF INFORMATION USED FOR GENERATING ENCRYPTION KEY
S10
EXCHANGE OF INFORMATION USED FOR GENERATING ENCRYPTION KEY
S11
EXCHANGE OF INFORMATION USED FOR GENERATING ENCRYPTION KEY
S12
GENERATE ENCRYPTION KEY
GENERATE ENCRYPTION KEY
SECURE DATA CHANNEL ESTABLISHED
APPLICATION DATA COMMUNICATION

FIG.2

FIG.3

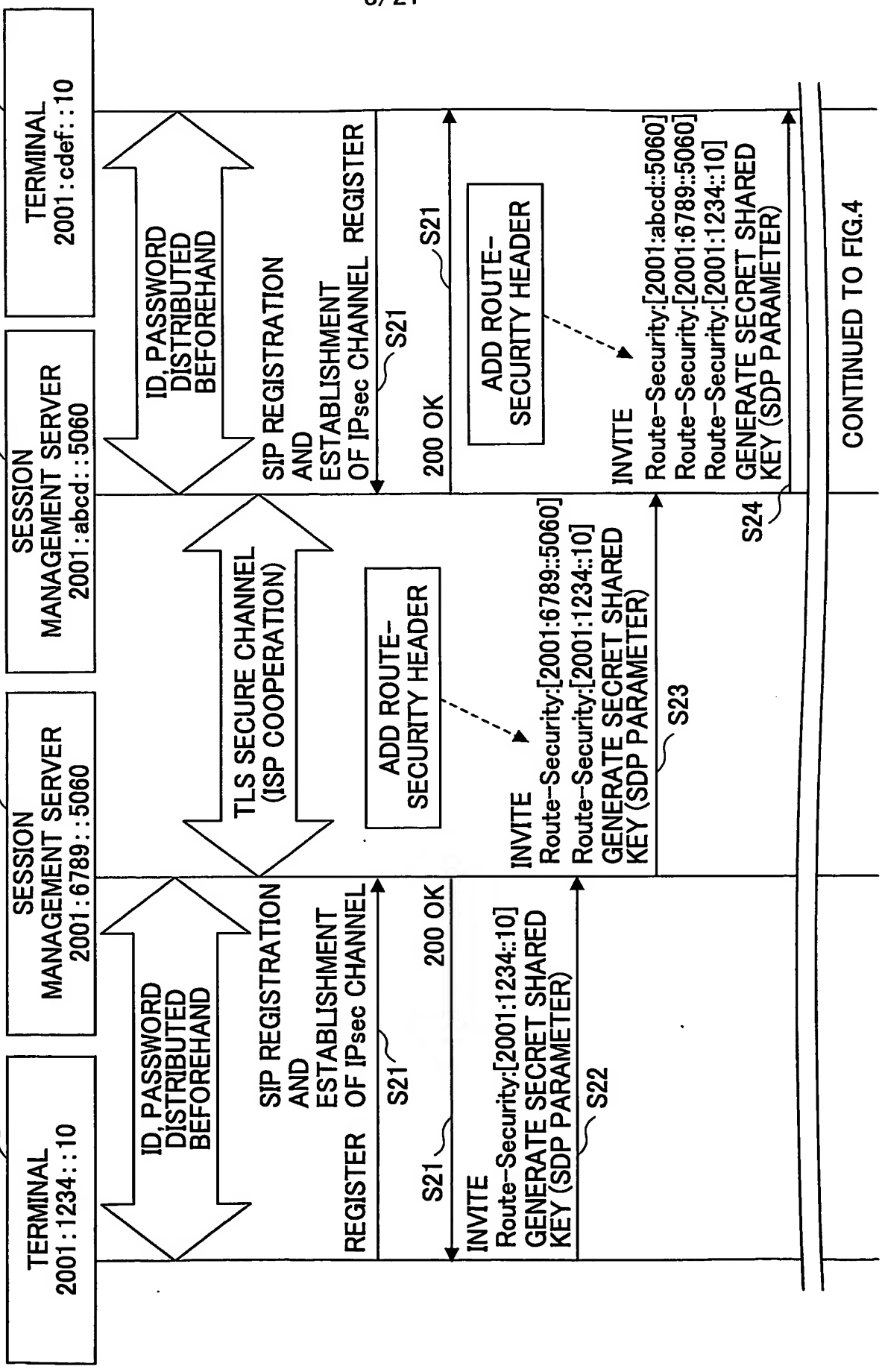

1
TERMINAL
2001:1234::10
A
SESSION
MANAGEMENT SERVER
2001:6789::5060
B
SESSION
MANAGEMENT SERVER
2001:abcd::5060
2
TERMINAL
2001:cdef::10
ID, PASSWORD
DISTRIBUTED
BEFOREHAND
SIP REGISTRATION
AND
ESTABLISHMENT
OF IPsec CHANNEL
REGISTER
S21
200 OK
S21
INVITE
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED
KEY (SDP PARAMETER)
S22
TLS SECURE CHANNEL
(ISP COOPERATION)
ADD ROUTE-
SECURITY HEADER
INVITE
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED
KEY (SDP PARAMETER)
S23
ADD ROUTE-
SECURITY HEADER
INVITE
Route-Security:[2001:abcd::5060]
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED
KEY (SDP PARAMETER)
S24
CONTINUED TO FIG.4

FIG.4

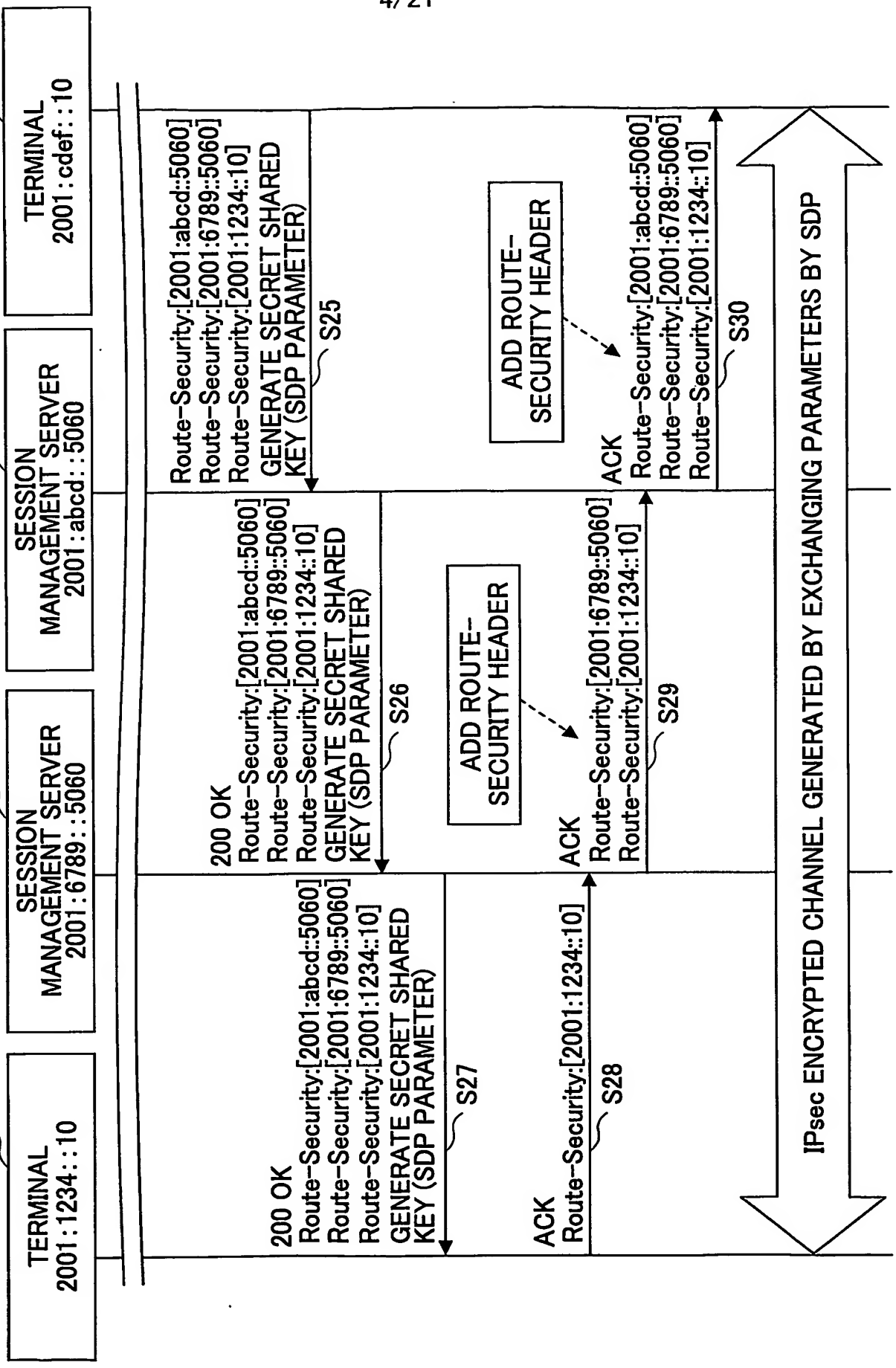
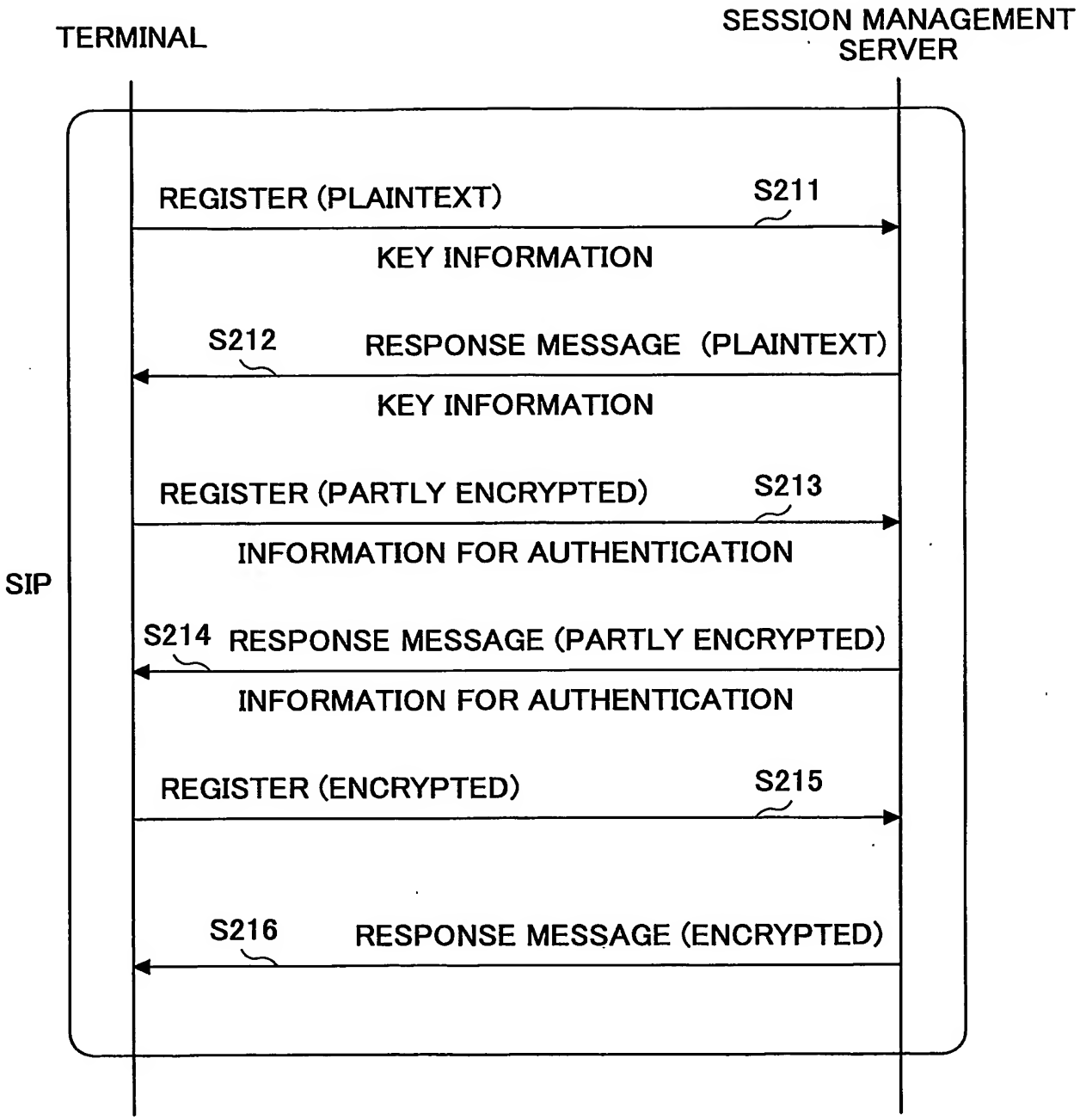

1
TERMINAL
2001:1234::10
A
SESSION
MANAGEMENT SERVER
2001:6789::5060
B
SESSION
MANAGEMENT SERVER
2001:abcd::5060
2
TERMINAL
2001:cdef::10
Route-Security:[2001:abcd::5060]
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED KEY (SDP PARAMETER)
S25
200 OK
Route-Security:[2001:abcd::5060]
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED KEY (SDP PARAMETER)
S26
ADD ROUTE-SECURITY HEADER
ACK
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
S29
ADD ROUTE-SECURITY HEADER
ACK
Route-Security:[2001:abcd::5060]
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
S30
200 OK
Route-Security:[2001:abcd::5060]
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
GENERATE SECRET SHARED KEY (SDP PARAMETER)
S27
ACK
Route-Security:[2001:1234::10]
S28
IPsec ENCRYPTED CHANNEL GENERATED BY EXCHANGING PARAMETERS BY SDP

FIG.5


TERMINAL
SESSION MANAGEMENT SERVER
SIP
REGISTER (PLAINTEXT)
S211
KEY INFORMATION
S212
RESPONSE MESSAGE (PLAINTEXT)
KEY INFORMATION
REGISTER (PARTLY ENCRYPTED)
S213
INFORMATION FOR AUTHENTICATION
S214
RESPONSE MESSAGE (PARTLY ENCRYPTED)
INFORMATION FOR AUTHENTICATION
REGISTER (ENCRYPTED)
S215
S216
RESPONSE MESSAGE (ENCRYPTED)

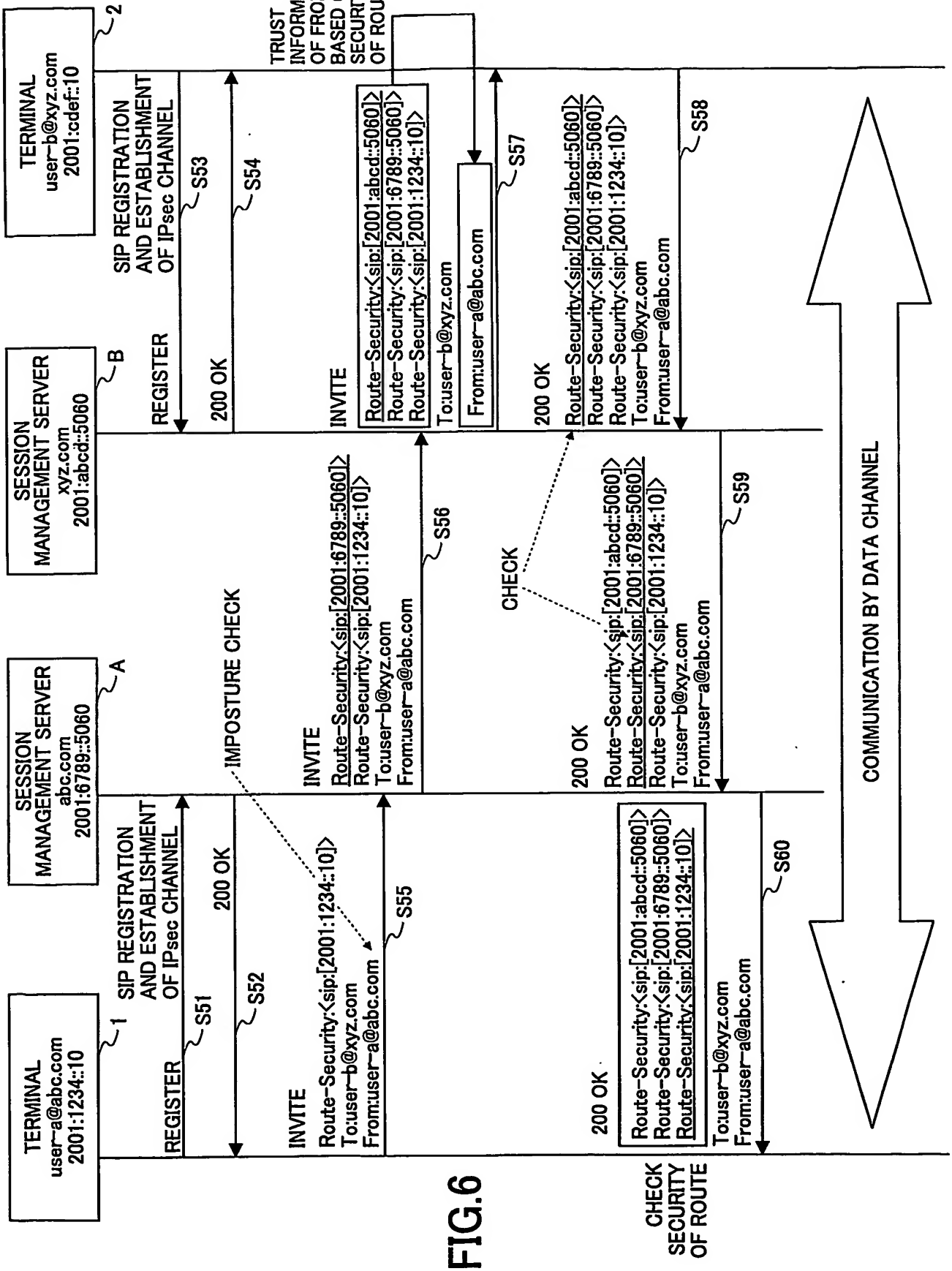

TERMINAL
user-a@abc.com
2001:1234::10
1
SESSION MANAGEMENT SERVER
abc.com
2001:6789::5060
A
SESSION MANAGEMENT SERVER
xyz.com
2001:abcd::5060
B
TERMINAL
user-b@xyz.com
2001:cdef::10
2
SIP REGISTRATION AND ESTABLISHMENT OF IPsec CHANNEL
REGISTER
S51
200 OK
S52
IMPOSTURE CHECK
INVITE
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S55
INVITE
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S56
SIP REGISTRATION AND ESTABLISHMENT OF IPsec CHANNEL
REGISTER
S53
200 OK
S54
TRUST INFORMATION OF FROM BASED ON SECURITY OF ROUTE
INVITE
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S57
CHECK
200 OK
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S58
200 OK
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S59
CHECK SECURITY OF ROUTE
200 OK
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:user-b@xyz.com
From:user-a@abc.com
S60
COMMUNICATION BY DATA CHANNEL

FIG.6

FIG.7

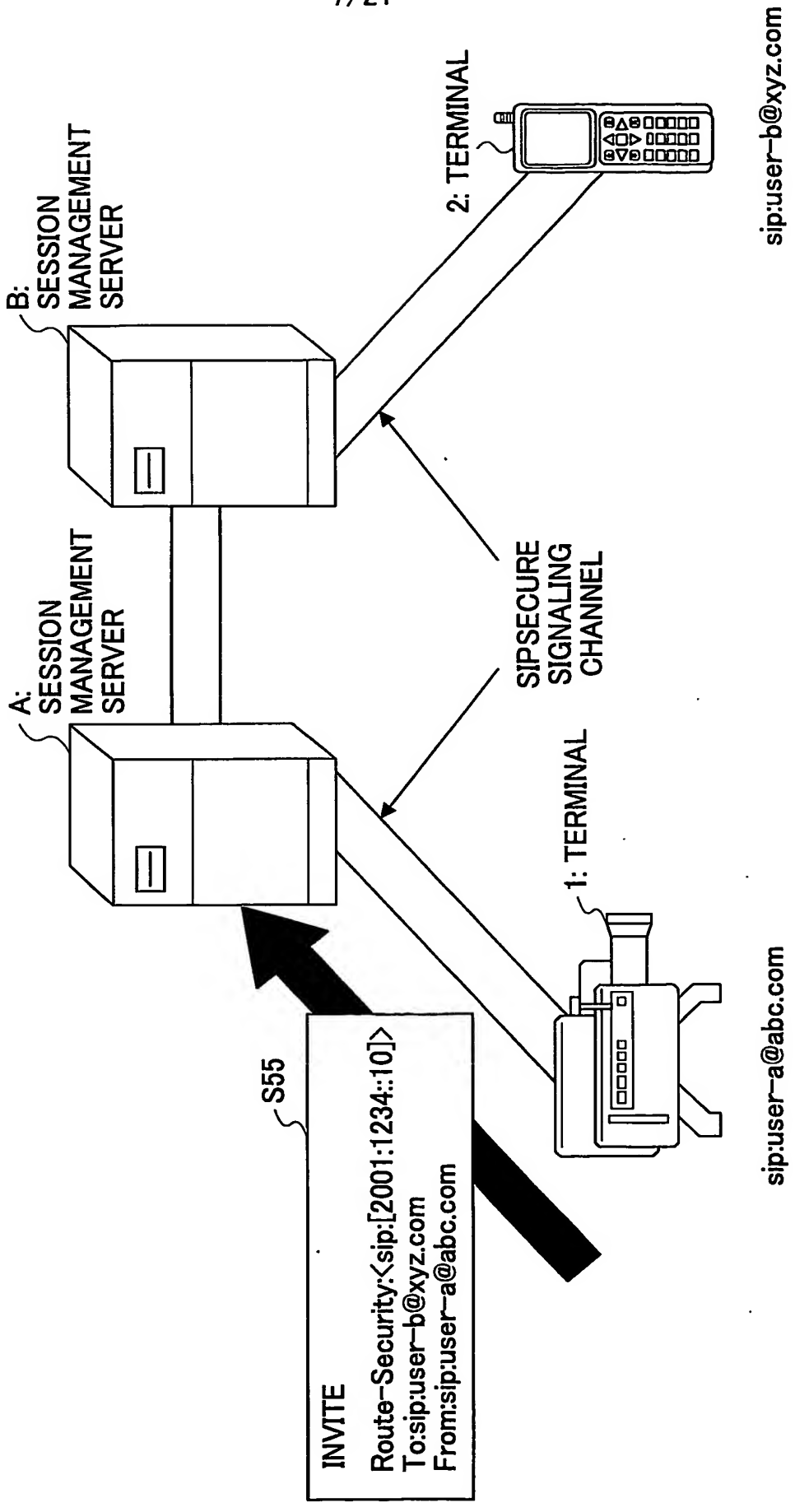

A: SESSION MANAGEMENT SERVER
B: SESSION MANAGEMENT SERVER
SIPSECURE SIGNALING CHANNEL
1: TERMINAL
2: TERMINAL
sip:user-a@abc.com
sip:user-b@xyz.com
S55
INVITE
Route-Security:<sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com

FIG.8

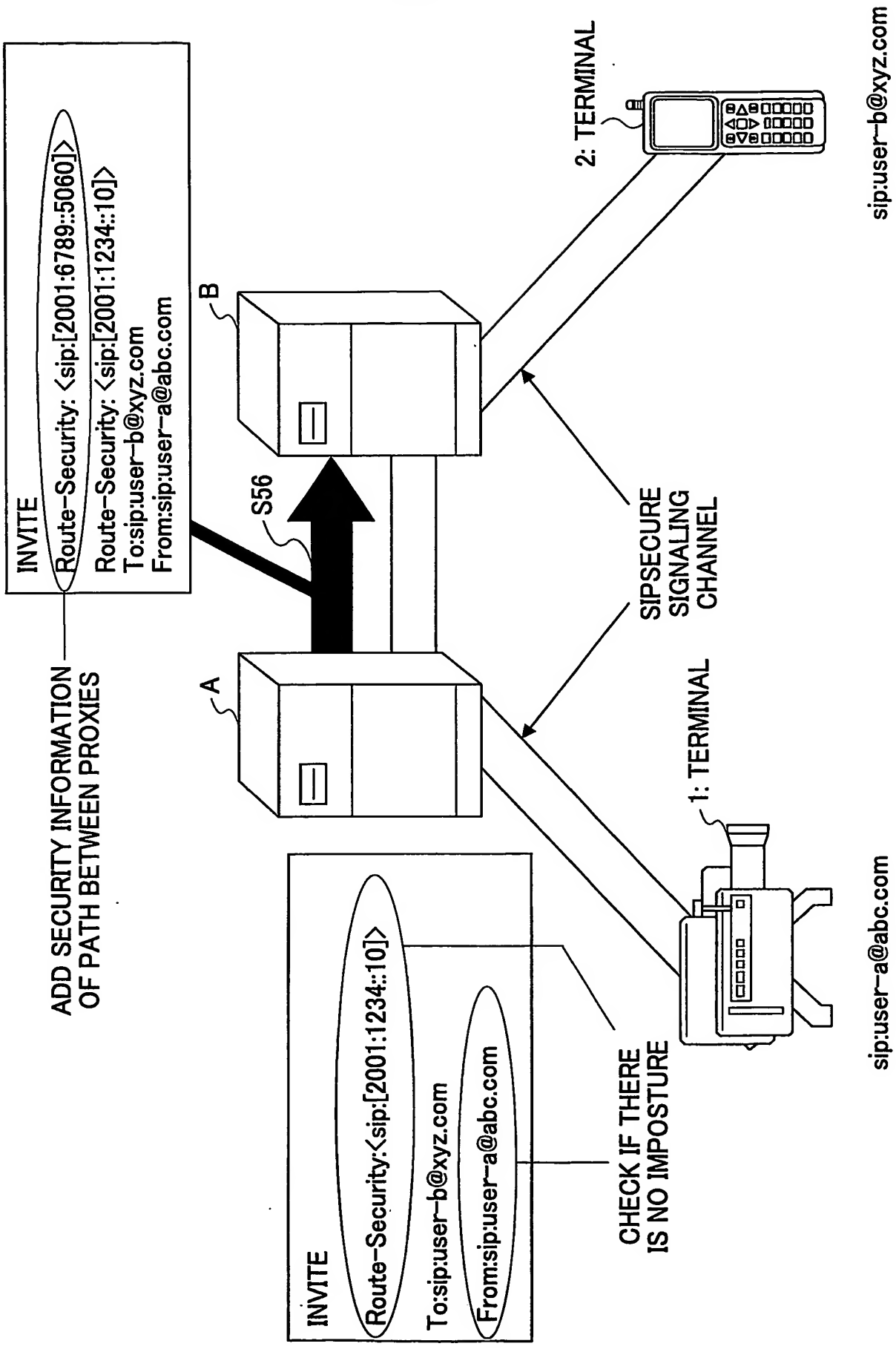

INVITE
Route-Security: <sip:[2001:6789::5060]>
Route-Security: <sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com
ADD SECURITY INFORMATION OF PATH BETWEEN PROXIES
S56
A
B
2: TERMINAL
1: TERMINAL
SIPSECURE SIGNALING CHANNEL
INVITE
Route-Security:<sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com
CHECK IF THERE IS NO IMPOSTURE
sip:user-b@xyz.com
sip:user-a@abc.com

FIG.9

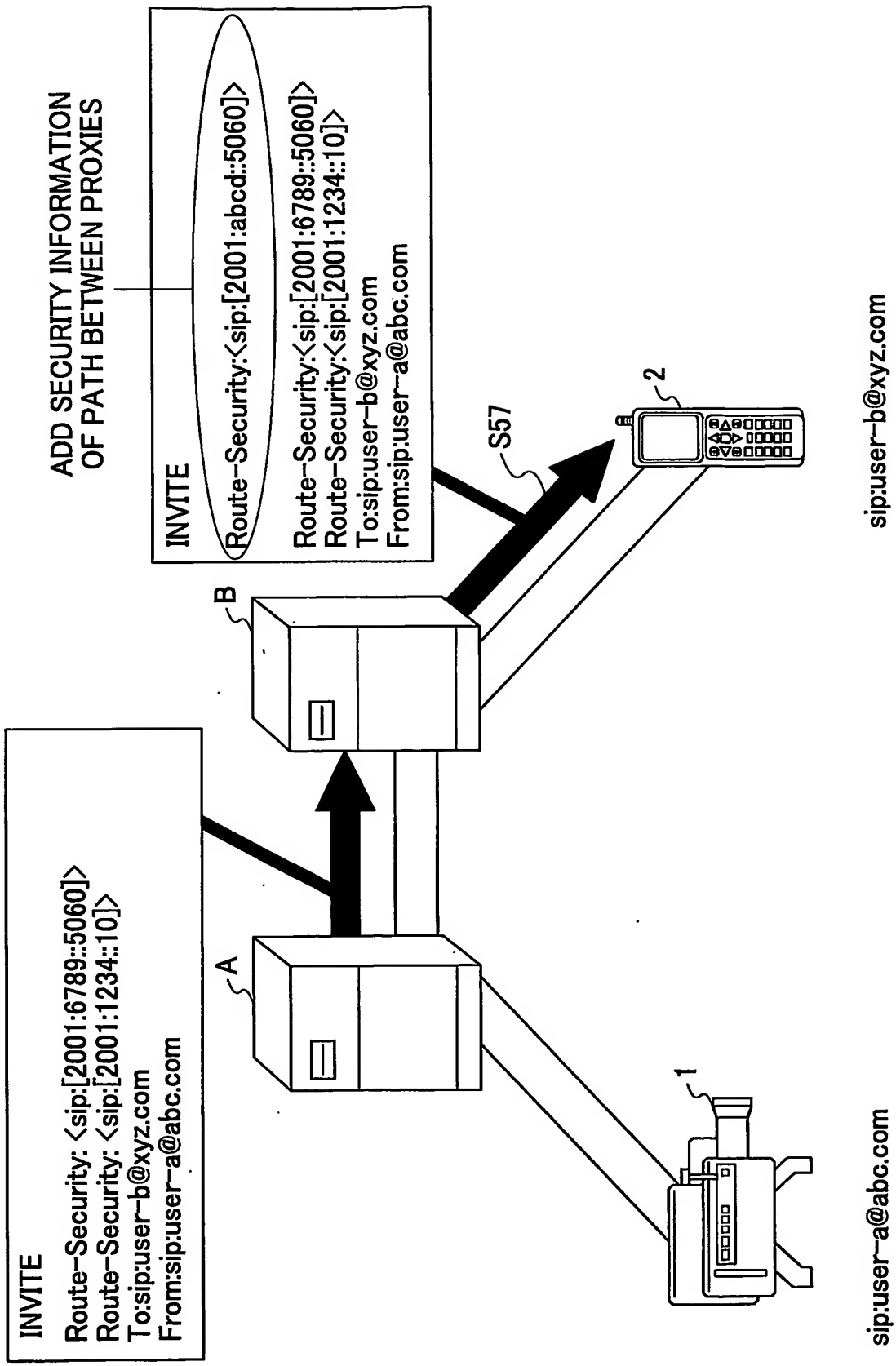

INVITE
Route-Security: <sip:[2001:6789::5060]>
Route-Security: <sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com
A
B
ADD SECURITY INFORMATION OF PATH BETWEEN PROXIES
INVITE
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com
S57
1
2
sip:user-a@abc.com
sip:user-b@xyz.com

FIG.10

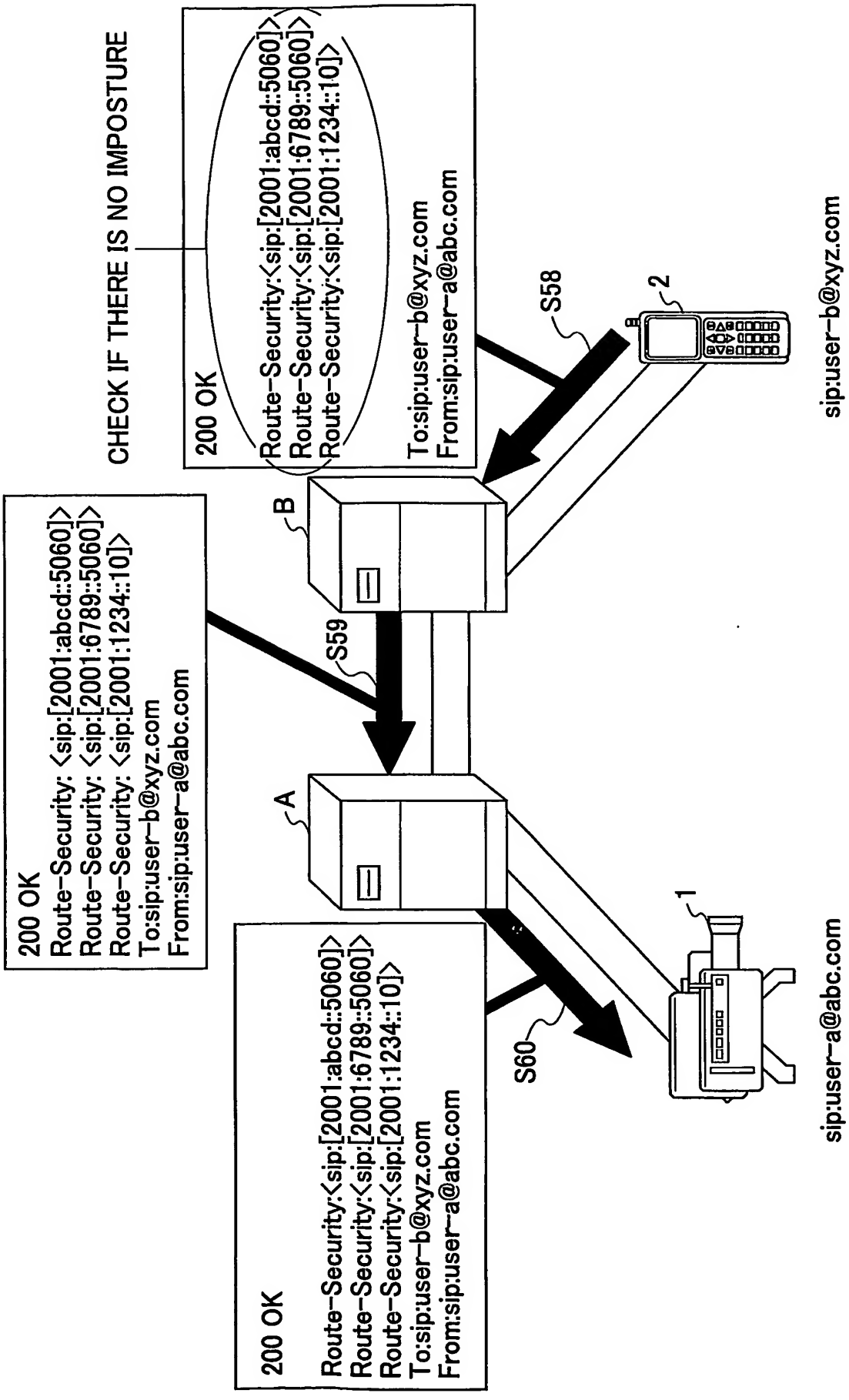

CHECK IF THERE IS NO IMPOSTURE
200 OK
Route-Security:<sip:[2001:abcd::5060]>
Route-Security:<sip:[2001:6789::5060]>
Route-Security:<sip:[2001:1234::10]>
To:sip:user-b@xyz.com
From:sip:user-a@abc.com
S58
S59
S60
A
B
1
2
sip:user-a@abc.com
sip:user-b@xyz.com

FIG.11

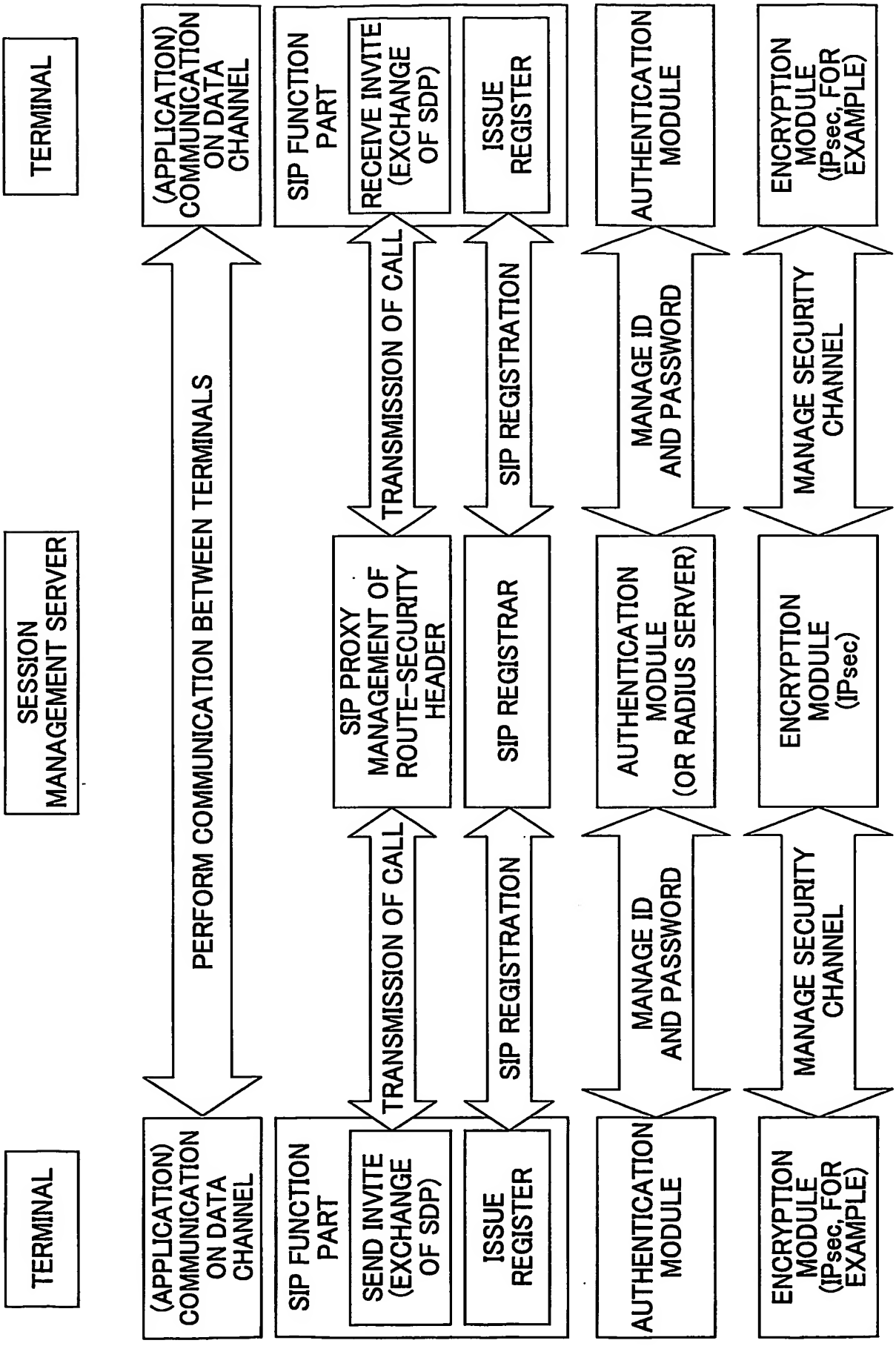

TERMINAL
SESSION MANAGEMENT SERVER
TERMINAL
(APPLICATION) COMMUNICATION ON DATA CHANNEL
SIP FUNCTION PART
SEND INVITE (EXCHANGE OF SDP)
ISSUE REGISTER
AUTHENTICATION MODULE
ENCRYPTION MODULE (IPsec, FOR EXAMPLE)
PERFORM COMMUNICATION BETWEEN TERMINALS
TRANSMISSION OF CALL
SIP REGISTRATION
MANAGE ID AND PASSWORD
MANAGE SECURITY CHANNEL
SIP PROXY MANAGEMENT OF ROUTE-SECURITY HEADER
SIP REGISTRAR
AUTHENTICATION MODULE (OR RADIUS SERVER)
ENCRYPTION MODULE (IPsec)
(APPLICATION) COMMUNICATION ON DATA CHANNEL
SIP FUNCTION PART
RECEIVE INVITE (EXCHANGE OF SDP)
ISSUE REGISTER
AUTHENTICATION MODULE
ENCRYPTION MODULE (IPsec, FOR EXAMPLE)

FIG.12

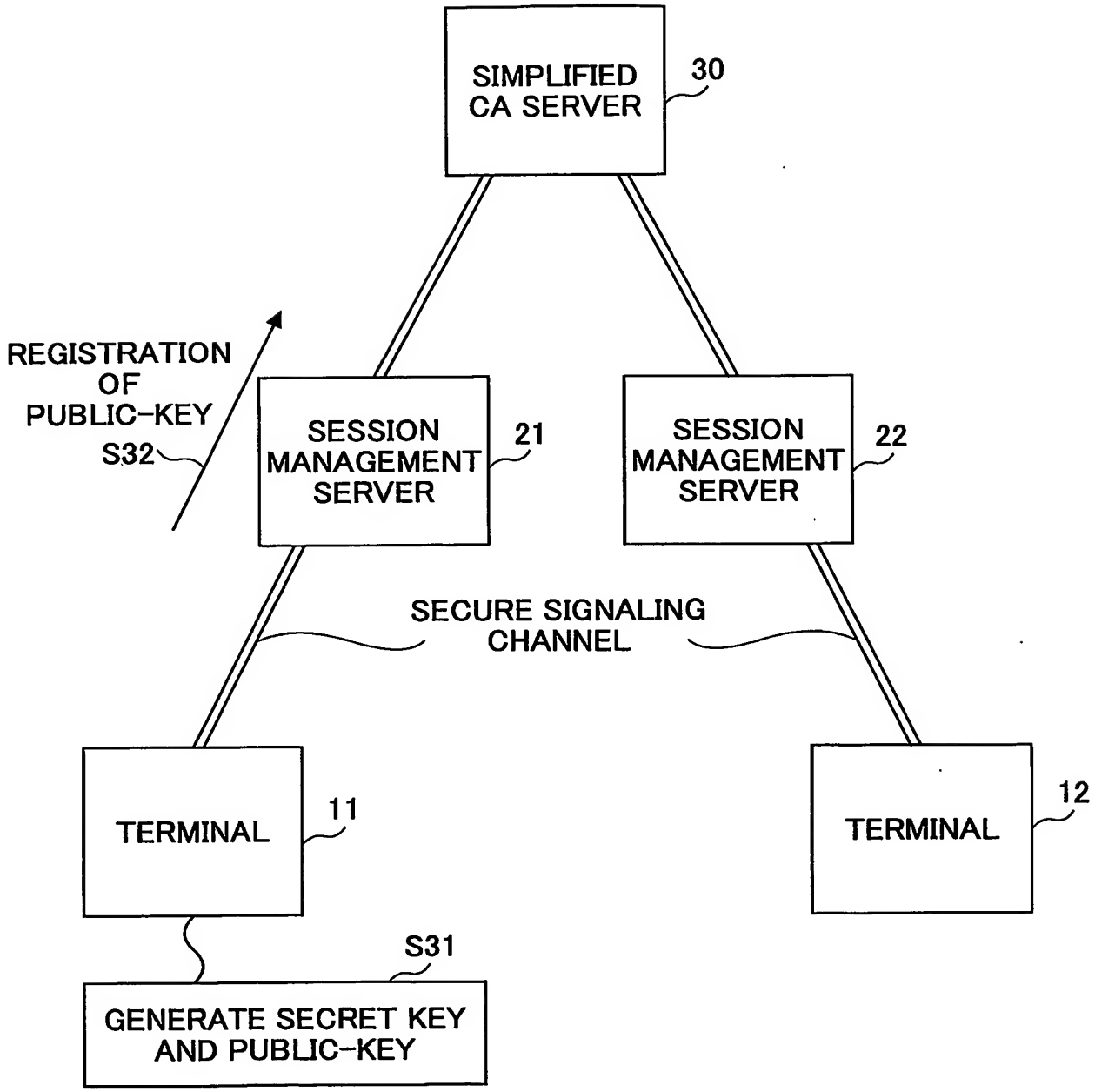

SIMPLIFIED CA SERVER
30
REGISTRATION OF PUBLIC-KEY
S32
SESSION MANAGEMENT SERVER
21
SESSION MANAGEMENT SERVER
22
SECURE SIGNALING CHANNEL
TERMINAL
11
TERMINAL
12
S31
GENERATE SECRET KEY AND PUBLIC-KEY

FIG.13

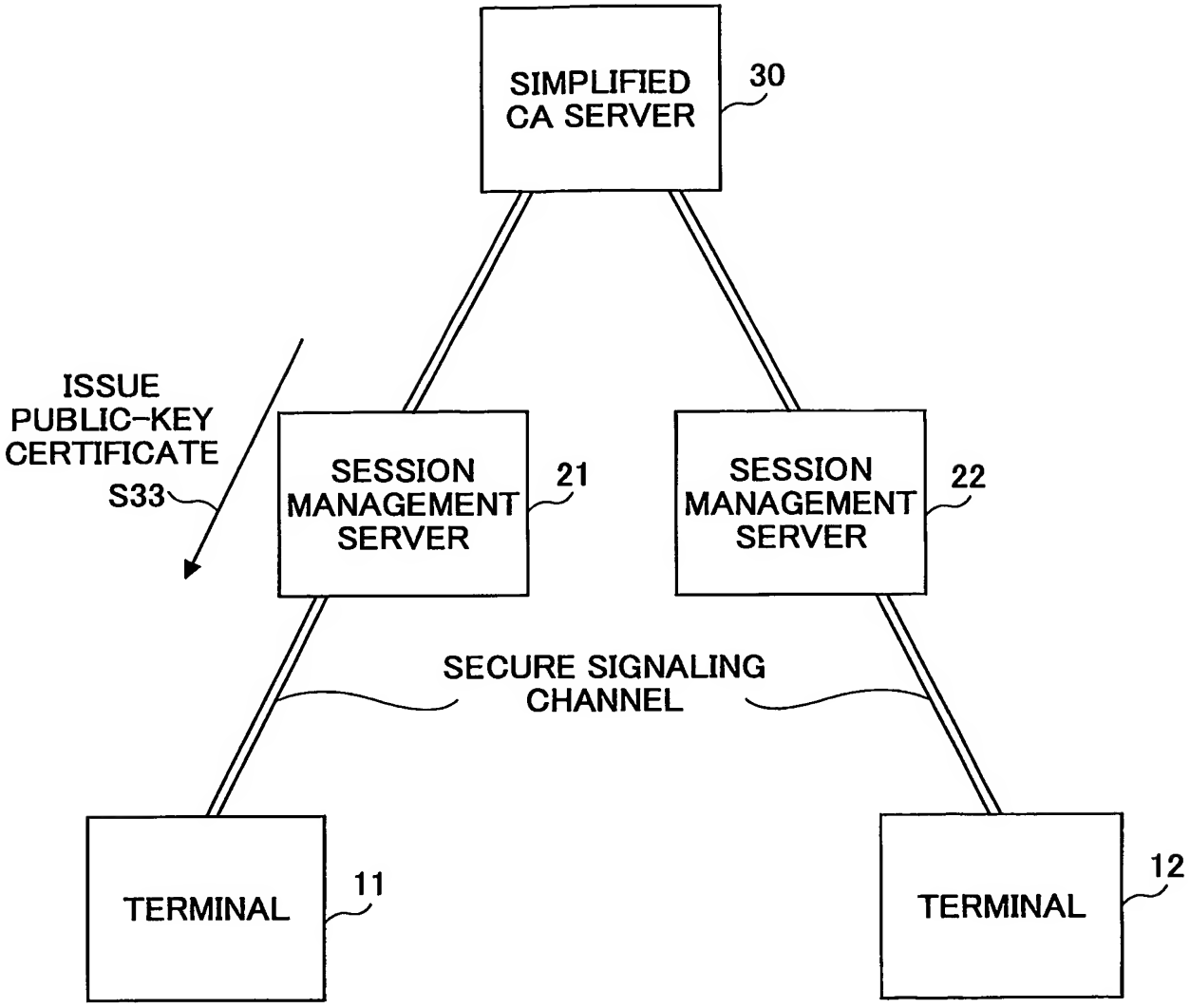

SIMPLIFIED CA SERVER
30
ISSUE PUBLIC-KEY CERTIFICATE
S33
SESSION MANAGEMENT SERVER
21
SESSION MANAGEMENT SERVER
22
SECURE SIGNALING CHANNEL
TERMINAL
11
TERMINAL
12

FIG.14

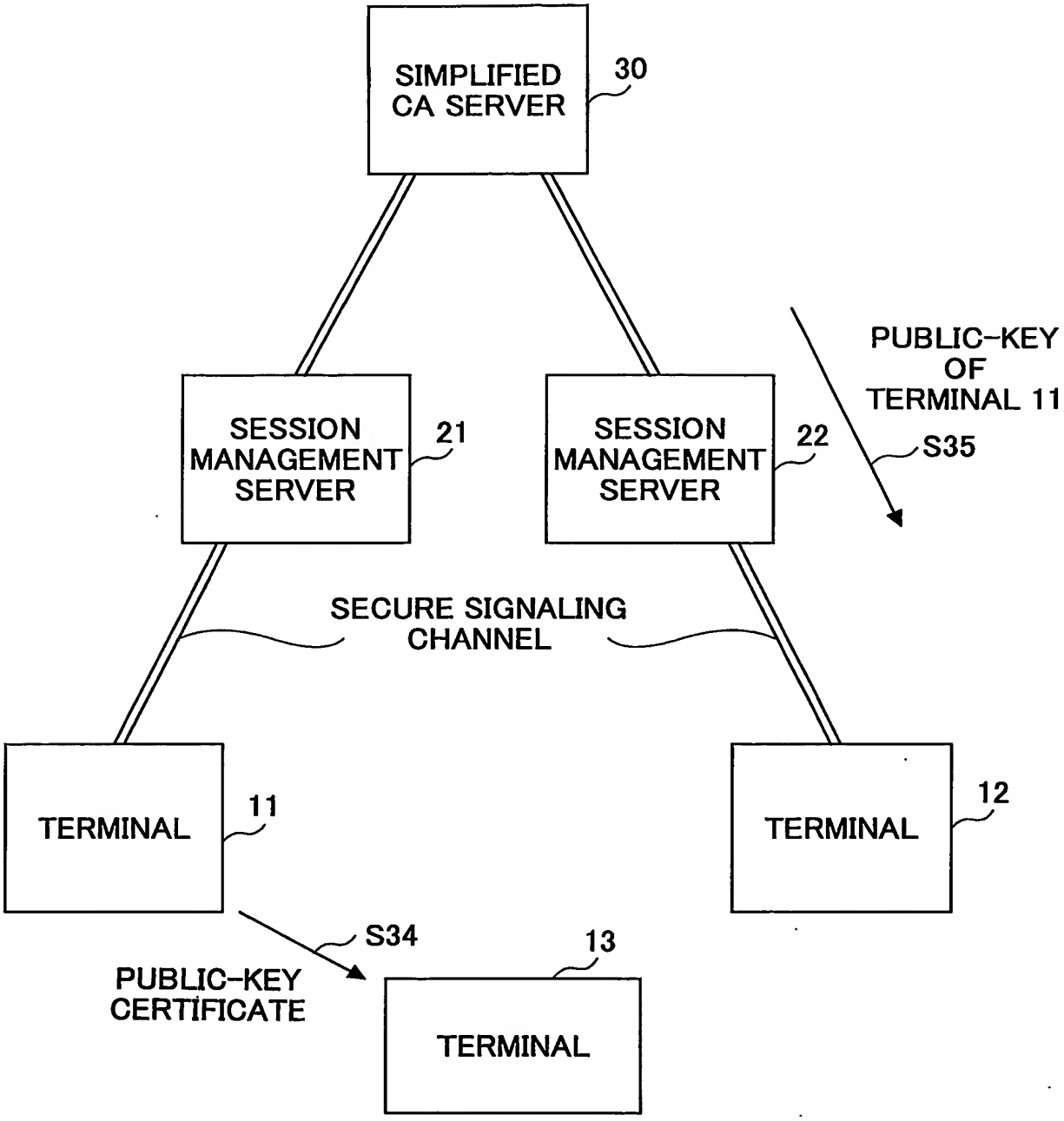

SIMPLIFIED CA SERVER
30
SESSION MANAGEMENT SERVER
21
SESSION MANAGEMENT SERVER
22
PUBLIC-KEY OF TERMINAL 11
S35
SECURE SIGNALING CHANNEL
TERMINAL
11
TERMINAL
12
S34
PUBLIC-KEY CERTIFICATE
13
TERMINAL

FIG.15

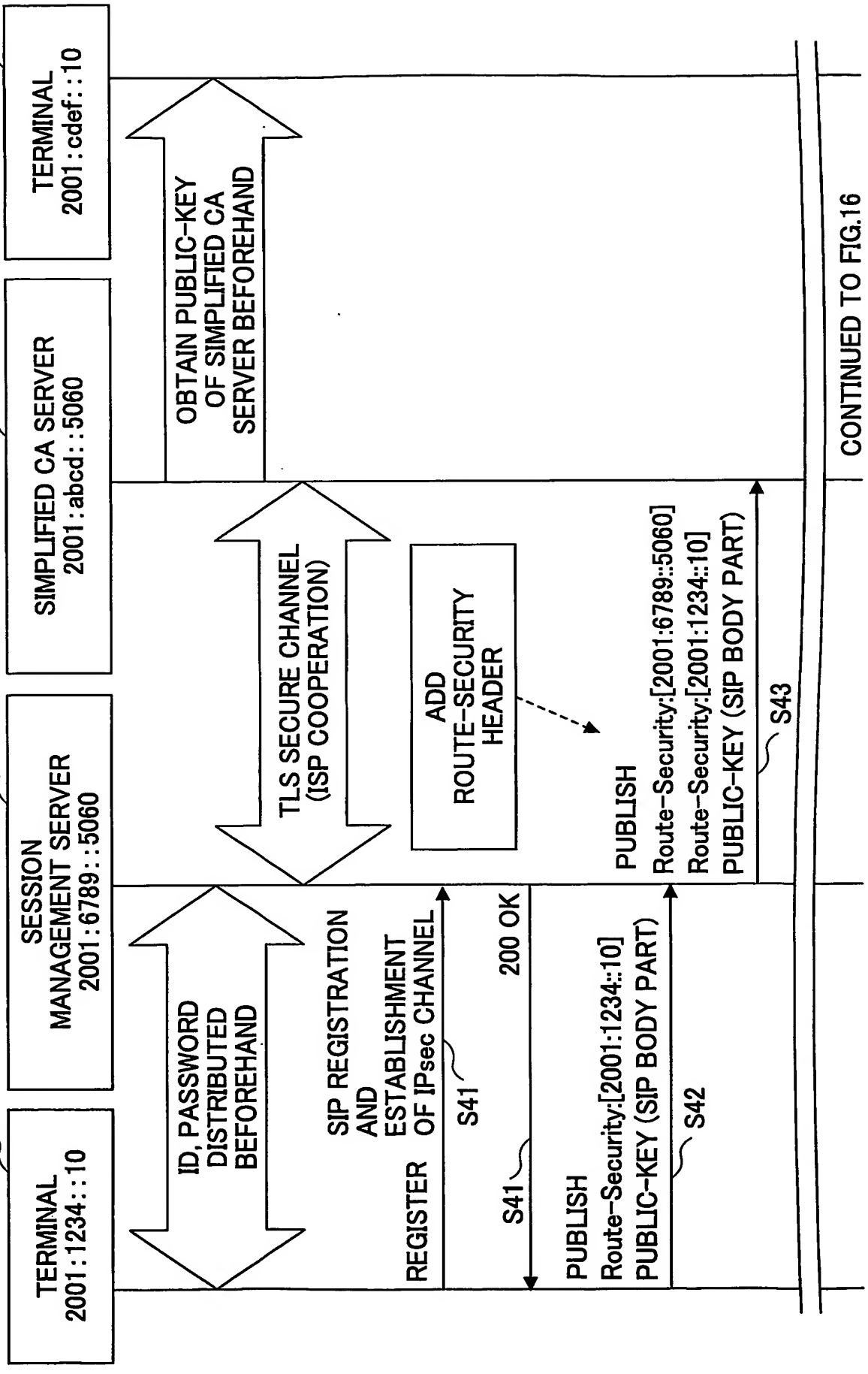

11
TERMINAL
2001:1234::10
21
SESSION
MANAGEMENT SERVER
2001:6789::5060
30
SIMPLIFIED CA SERVER
2001:abcd::5060
13
TERMINAL
2001:cdef::10
ID, PASSWORD
DISTRIBUTED
BEFOREHAND
OBTAIN PUBLIC-KEY
OF SIMPLIFIED CA
SERVER BEFOREHAND
TLS SECURE CHANNEL
(ISP COOPERATION)
SIP REGISTRATION
AND
ESTABLISHMENT
OF IPsec CHANNEL
REGISTER
S41
200 OK
S41
ADD
ROUTE-SECURITY
HEADER
PUBLISH
Route-Security:[2001:1234::10]
PUBLIC-KEY (SIP BODY PART)
S42
PUBLISH
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
PUBLIC-KEY (SIP BODY PART)
S43
CONTINUED TO FIG.16

FIG.16

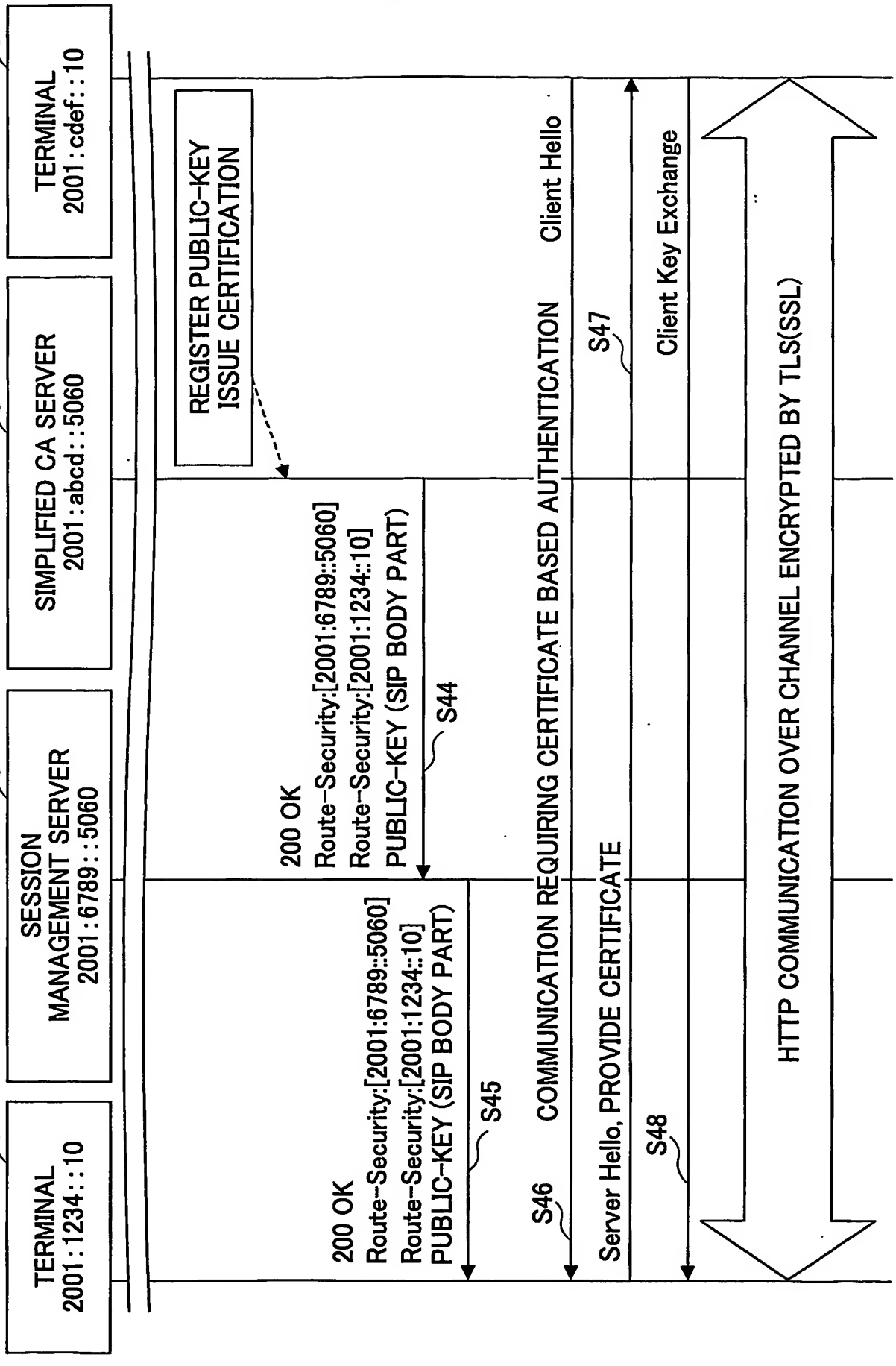

11
TERMINAL
2001:1234::10
21
SESSION
MANAGEMENT SERVER
2001:6789::5060
30
SIMPLIFIED CA SERVER
2001:abcd::5060
13
TERMINAL
2001:cdef::10
REGISTER PUBLIC-KEY
ISSUE CERTIFICATION
200 OK
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
PUBLIC-KEY (SIP BODY PART)
S44
200 OK
Route-Security:[2001:6789::5060]
Route-Security:[2001:1234::10]
PUBLIC-KEY (SIP BODY PART)
S45
S46
COMMUNICATION REQUIRING CERTIFICATE BASED AUTHENTICATION
Client Hello
S47
Server Hello, PROVIDE CERTIFICATE
Client Key Exchange
S48
HTTP COMMUNICATION OVER CHANNEL ENCRYPTED BY TLS(SSL)

FIG.17

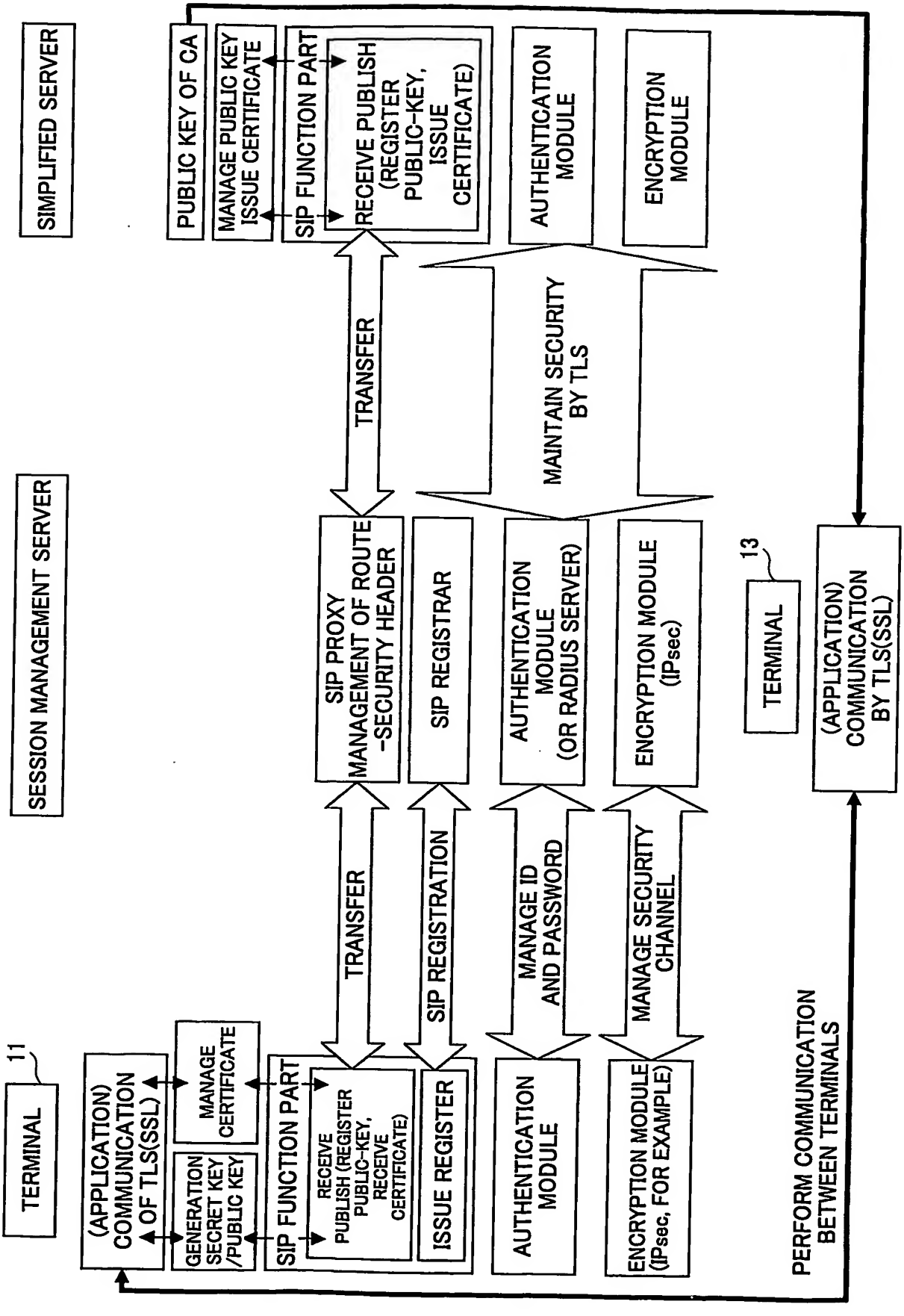

SIMPLIFIED SERVER
PUBLIC KEY OF CA
MANAGE PUBLIC KEY ISSUE CERTIFICATE
SIP FUNCTION PART
RECEIVE PUBLISH (REGISTER PUBLIC-KEY, ISSUE CERTIFICATE)
AUTHENTICATION MODULE
ENCRYPTION MODULE
TRANSFER
MAINTAIN SECURITY BY TLS
SESSION MANAGEMENT SERVER
SIP PROXY MANAGEMENT OF ROUTE -SECURITY HEADER
SIP REGISTRAR
AUTHENTICATION MODULE (OR RADIUS SERVER)
ENCRYPTION MODULE (IPsec)
13
TERMINAL
(APPLICATION) COMMUNICATION BY TLS(SSL)
TRANSFER
SIP REGISTRATION
MANAGE ID AND PASSWORD
MANAGE SECURITY CHANNEL
11
TERMINAL
(APPLICATION) COMMUNICATION OF TLS(SSL)
MANAGE CERTIFICATE
GENERATION SECRET KEY /PUBLIC KEY
SIP FUNCTION PART
RECEIVE PUBLISH (REGISTER PUBLIC-KEY, RECEIVE CERTIFICATE)
ISSUE REGISTER
AUTHENTICATION MODULE
ENCRYPTION MODULE (IPsec, FOR EXAMPLE)
PERFORM COMMUNICATION BETWEEN TERMINALS

FIG.18

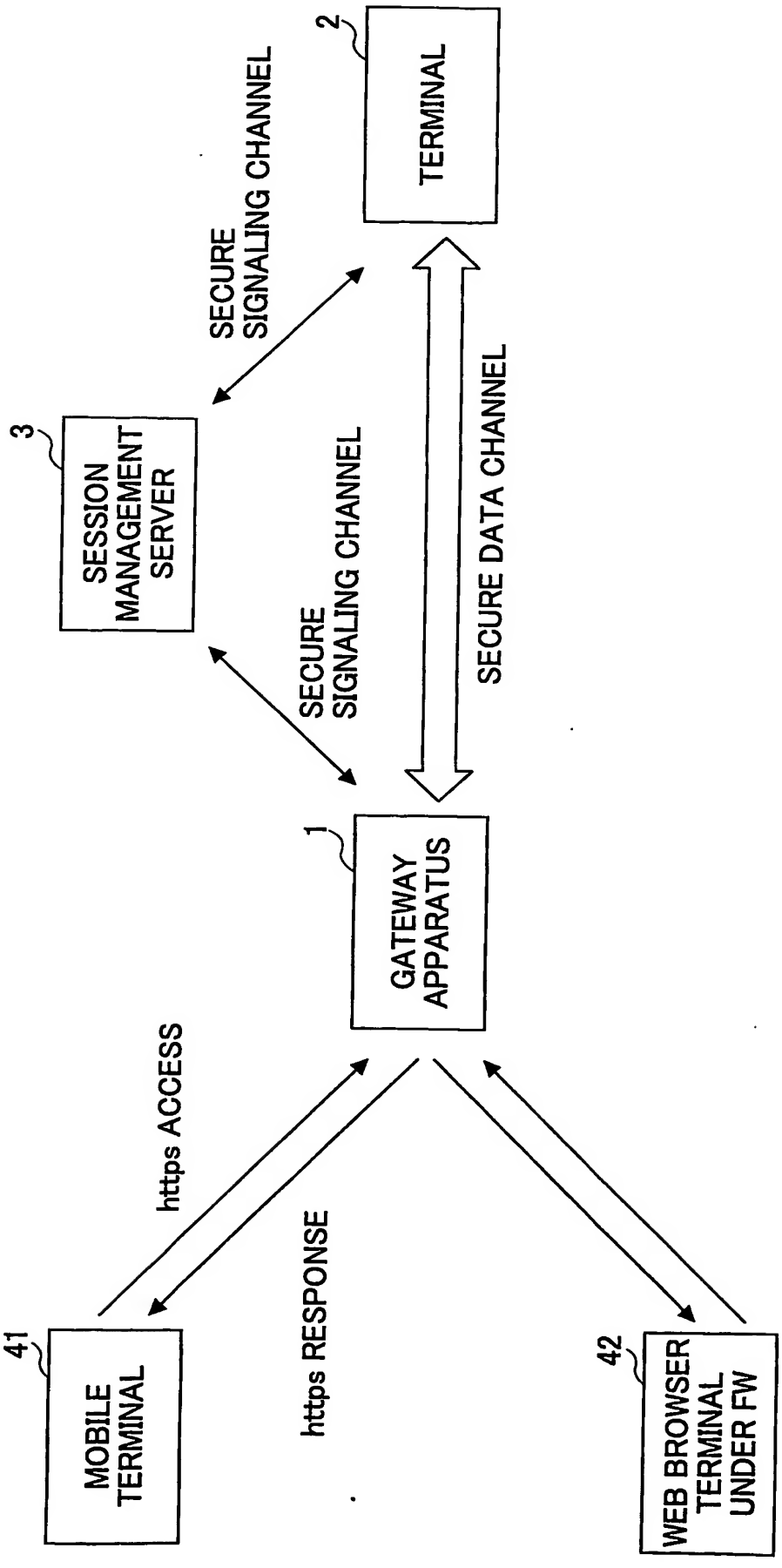

2
TERMINAL
SECURE SIGNALING CHANNEL
3
SESSION MANAGEMENT SERVER
SECURE SIGNALING CHANNEL
SECURE DATA CHANNEL
1
GATEWAY APPARATUS
https ACCESS
https RESPONSE
41
MOBILE TERMINAL
42
WEB BROWSER TERMINAL UNDER FW

FIG.19

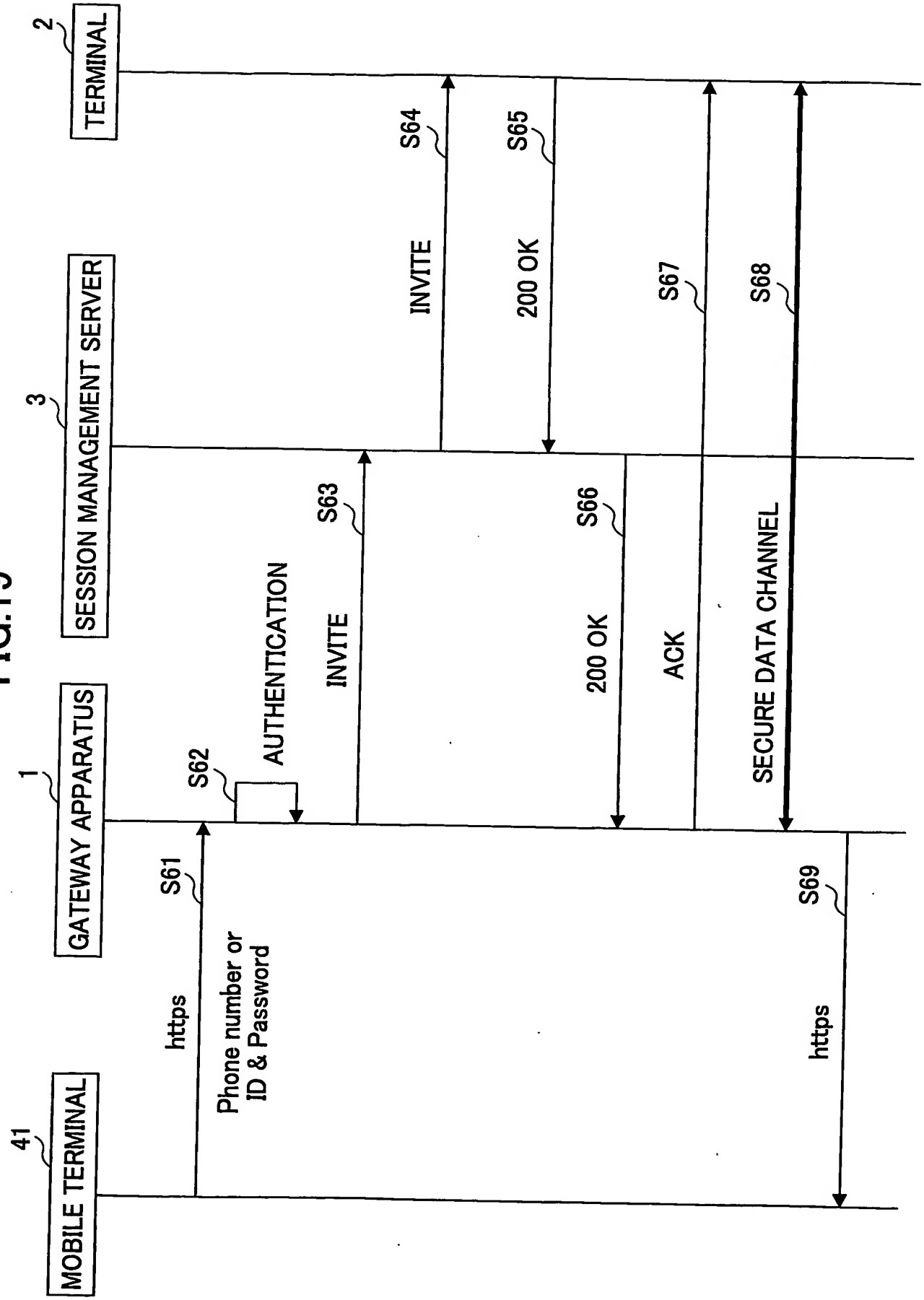
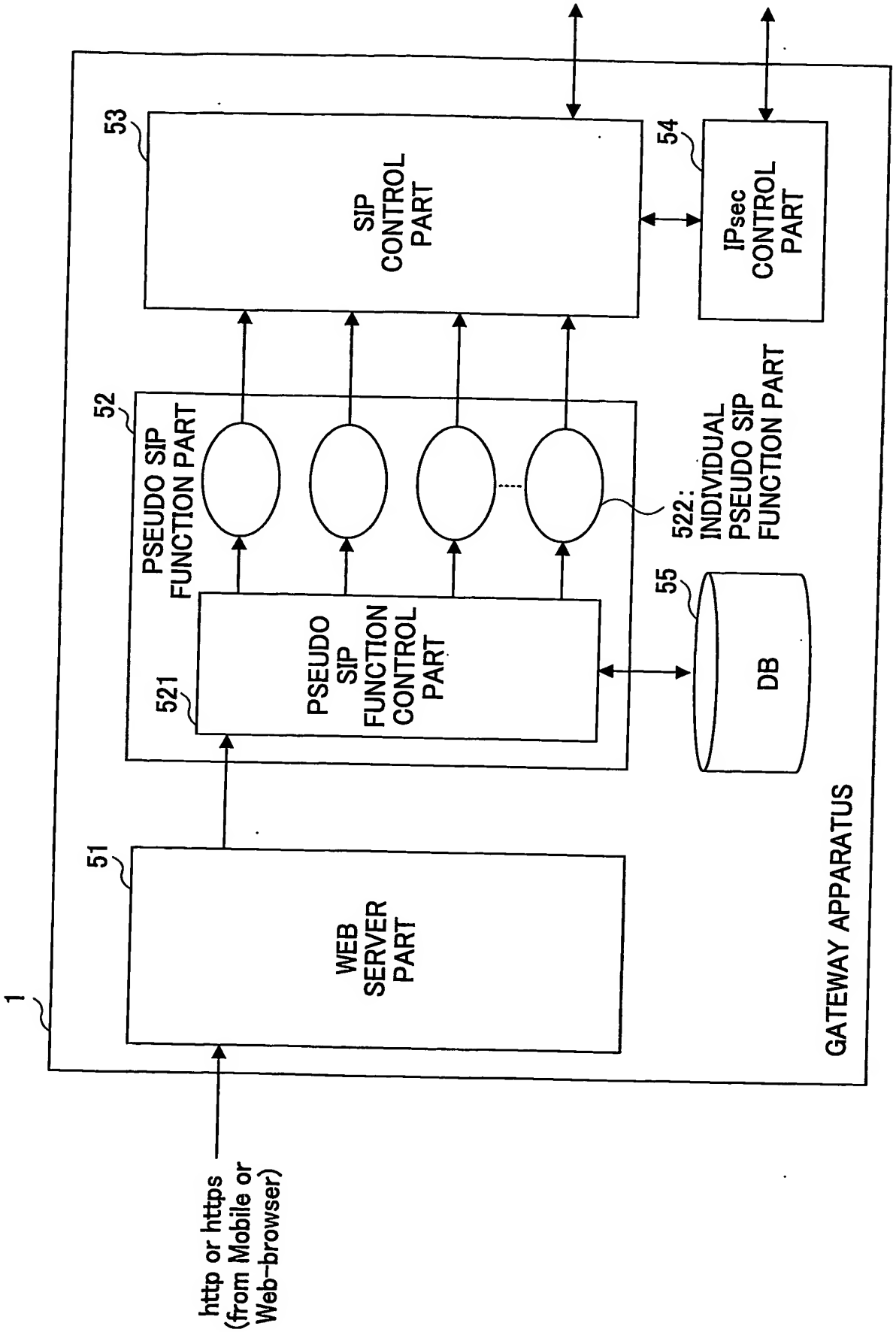

MOBILE TERMINAL
41
GATEWAY APPARATUS
1
SESSION MANAGEMENT SERVER
3
TERMINAL
2
S61
https
Phone number or ID & Password
S62
AUTHENTICATION
S63
INVITE
S64
INVITE
S65
200 OK
S66
200 OK
S67
ACK
S68
SECURE DATA CHANNEL
S69
https

FIG.20

USER IDENTIFIER	NAME OF ACCESS DESTINATION
× × ×	AAA,BBB,CCC,・・・・・
⋮	⋮

FIG.21


1
GATEWAY APPARATUS
51
WEB SERVER PART
52
PSEUDO SIP FUNCTION PART
521
PSEUDO SIP FUNCTION CONTROL PART
522: INDIVIDUAL PSEUDO SIP FUNCTION PART
53
SIP CONTROL PART
54
IPsec CONTROL PART
55
DB
http or https (from Mobile or Web-browser)